

U.S. Application No. 10/786,072

**REMARKS****RECEIVED  
CENTRAL FAX CENTER****APR 03 2008**

The Applicants request reconsideration of the rejection.

The Applicants' representative thanks the Examiner for the courtesies extended during various telephone conferences, during which a draft of this paper was discussed. It is the understanding of the representative that the application will be in condition for allowance upon entry of the above amendments.

Claims 17 and 29-32 remain pending. Claim 32 is a new claim, described, by way of illustrative example, by the access interception process found on pages 14-15 of the present specification.

Claims 17 and 29-31 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Chebolu, U.S. Patent Publication No. 2005/0065935 (Chebolu) in view of Costa-Requena et al., U.S. Patent Publication No. 2004/0221037 (Costa-Requena) in view of Weber, U.S. Patent Publication No. 2002/0184360 (Weber).

The Applicants traverse as follows.

Although Chebolu is not established as prior art to the present application, the Applicants believe that the pending claims can be distinguished most easily by noting deficiencies in Costa-Requena, as applied in the Office Action. In particular, Costa-Requena is recited as disclosing that the access prohibited user list is referenced prior to the access control list, such that in combination with Chebolu, the updating and/or synchronizing of access control lists, as claimed, is disclosed. However, according to Costa-Requena, both the deny list and allow list must be checked in order to deny a requested access. In particular, the deny list is first checked, and if the user appears on the deny list, the allow list is still checked to find out if the user appears in the allow list. Because allowance is the default, if the user

appears on the allow list, then access is permitted. Access is only denied if a user appears on the deny list and not on the allow list, due to the default allowance.

According to the present invention, on the other hand, if the user information is found on the access prohibited list, then access is intercepted without checking the access control list. To emphasize this feature of the invention, independent claim 17 has been amended to recite that the access interception module is configured to intercept the access by reference to the access prohibition list of the access controller, which records user information of access prohibited users prior to referencing the access control list by the access restriction module.

In addition, claim 17 has been amended to recite other features not found in the references of record. In particular, claim 17 now recites that the distribution module of at least one of the access controllers having received user information to be added to the access prohibition list thereof, and an access prohibition list updated accordingly is configured to send out the user information added to the updated access prohibition list or the entire updated access prohibition list to the other access controllers in response to the access prohibition list of the sending access controller being updated. Thus, according to the invention, when a user is newly entered to the access prohibition list, the user information of the user is added to the access prohibition list and the distribution module sends either the added user information or the entire updated access prohibition list to the other access controllers. This permits quick interception of any access attempted by the blacklisted user.

Claim 17 has also been amended to recite that, after the list update module of each of the receiving access controllers updates its access prohibition list, the access control list update module thereof updates the access control list thereof

according to the updated access prohibition list thereof, removing access rights from the access control list for any user corresponding to the user information in the updated access prohibition list. By this feature, the access rights of the blacklisted user are removed from the access control list, according to the update. While this feature may have been understood in the rejected claim, the amendment is believed to clarify the feature.

Claim 17 has also been amended to recite that after completing the updating of the access control list, each of the other access controllers deletes the received user information from its updated access prohibition list or deletes the entire updated access prohibition list. This feature is also absent from the art of record.

New claim 32 recites a feature in which access by a blacklisted user is deleted from an access management table, for any user whose information is added the access prohibition list. By this feature, even accesses in progress can be intercepted according to the invention.

In view of the foregoing amendments and remarks, the Applicants request reconsideration of the rejection and allowance of the claims.

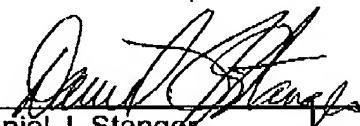
To the extent necessary, the Applicants petition for an extension of time under 37 CFR 1.136. Please charge any shortage in fees due in connection with the filing of this paper, including extension of time fees, or credit any overpayment of fees, to

U.S. Application No. 10/786,072

the deposit account of Mattingly, Stanger, Malur & Brundidge, P.C., Deposit Account No. 50-1417 (referencing attorney docket no. MEI-101).

Respectfully submitted,

MATTINGLY, STANGER, MALUR & BRUNDIDGE, P.C.

  
\_\_\_\_\_  
Daniel J. Stanger  
Registration No. 32,846

DJS/sdb  
(703) 684-1120